

Math 261, Number Theory — Fall 2009–2010
Course website: <http://people.aub.edu.lb/~kmakdisi/>
Problem set 3, due Friday, October 30 at the beginning of class

Exercise 3.1: Assume that $\bar{a} \in (\mathbf{Z}/m\mathbf{Z})^*$ has multiplicative order k . Let $\ell \in \mathbf{Z}$, and take $\bar{b} = \bar{a}^\ell$.

- a) If $(k, \ell) = 1$, show that \bar{b} also has order k .
- b) In general, even if k and ℓ are not relatively prime, what is the order of \bar{b} ?
- c) Coming back to the case where $(k, \ell) = 1$, show that in this case \bar{a} can be written as a power of \bar{b} (i.e., $\bar{a} = \bar{b}^n$ for some n).

d) Application of part (c): Show that for all $\bar{b} \in (\mathbf{Z}/101\mathbf{Z})^*$, there exists a **unique** $\bar{a} \in (\mathbf{Z}/101\mathbf{Z})^*$ such that $\bar{b} = \bar{a}^3$. Thus \bar{a} is the “cube root” of \bar{b} . For example, if $\bar{b} = \overline{14}$, then we have $\bar{a} = \overline{6}$, since $6^3 = 216 \equiv 14 \pmod{101}$.

Cultural remark: for general $(\mathbf{Z}/p\mathbf{Z})^*$, cube roots may or may not exist, and they may or may not be unique. Work out for yourselves the situation mod 13.

Exercise 3.2: 1) Suppose given numbers a and m , such that

$$a^{360} \equiv 1 \pmod{m}, \quad a^{180} \not\equiv 1 \pmod{m}, \quad a^{120} \not\equiv 1 \pmod{m}, \quad a^{72} \not\equiv 1 \pmod{m}.$$

Show that the order of $a \pmod{m}$ is exactly 360. (Hint: $360 = 2^3 3^2 5$, $180 = 360/2$, $120 = 360/3$, and $72 = 360/5$.)

2) Formulate and prove a general theorem giving a criterion for a to have order $k \pmod{m}$, under conditions similar to those in part 1.

Exercise 3.3: If p is a prime other than 2 or 5, show that p divides infinitely many numbers of the form

$$11, 111, 1111, 11111, 111111, 1111111, \dots$$

Suggestion: this is easy if $p = 3$. Otherwise, consider the multiplicative order of $10 \pmod{p}$.

Exercise 3.4: 1) Find $\phi(101)$, $\phi(6561)$, and $\phi(25200)$.

2) Compute the remainder of 2^{705} when divided by 101, and the remainder of 11^{17282} when divided by 25200.

Exercise 3.5: Here is another proof of the “existence” part of the Chinese Remainder Theorem: given m, n which are relatively prime, and any a, b , then there **exists** an x satisfying the simultaneous congruences

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n} \tag{*}$$

(Recall that the solution will be unique mod mn , but I’m not asking you to prove this.)

a) Show directly that if m and n are relatively prime, then there exist numbers v and w such that

$$\begin{cases} v \equiv 1 \pmod{m} \\ v \equiv 0 \pmod{n} \end{cases}, \quad \begin{cases} w \equiv 0 \pmod{m} \\ w \equiv 1 \pmod{n} \end{cases} \tag{**}$$

b) Use v, w, a , and b to produce a solution x to the equation (*).

c) Let $m = 12$ and $n = 203$, and find v and w satisfying equations (**). Use this to find $x \pmod{2436}$ satisfying $x \equiv 3 \pmod{12}$ and $x \equiv 5 \pmod{203}$.

Exercise 3.6: 1) Show that 1729 is a Carmichael number.

2) Use the Chinese Remainder Theorem to find all the solutions of the equation $x^2 \equiv 1 \pmod{1729}$. (This is unrelated to part 1, except for the fact that you need to know the factorization of 1729.)